



The Printer Working Group

~~August xx~~November 1, 2014
Working Draft

Imaging Device Security Identification, Authentication and Authorization (IDS-IAA)

Status: Initial

Abstract: This standard defines a set of requirements, methods, and data models for defining and sharing security identification, authentication and authorization information between various imaging services, devices and users.

This document is a PWG Working Draft. For a definition of a "PWG Working Draft", see: <ftp://ftp.pwg.org/pub/pwg/general/pwg-process30.pdf>

This document is available electronically at:

<ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20140804.pdf>

1 Copyright © 2014 The Printer Working Group. All rights reserved.

2 This document may be copied and furnished to others, and derivative works that comment
3 on, or otherwise explain it or assist in its implementation may be prepared, copied,
4 published and distributed, in whole or in part, without restriction of any kind, provided that
5 the above copyright notice, this paragraph and the title of the Document as referenced
6 below are included on all such copies and derivative works. However, this document itself
7 may not be modified in any way, such as by removing the copyright notice or references to
8 the IEEE-ISTO and the Printer Working Group, a program of the IEEE-ISTO.

9 Title: *IDS Identification, Authentication and Authorization (IDS-IAA)*

10 The IEEE-ISTO and the Printer Working Group DISCLAIM ANY AND ALL WARRANTIES,
11 WHETHER EXPRESS OR IMPLIED INCLUDING (WITHOUT LIMITATION) ANY IMPLIED
12 WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

13 The Printer Working Group, a program of the IEEE-ISTO, reserves the right to make
14 changes to the document without further notice. The document may be updated, replaced
15 or made obsolete by other documents at any time.

16 The IEEE-ISTO takes no position regarding the validity or scope of any intellectual
17 property or other rights that might be claimed to pertain to the implementation or use of the
18 technology described in this document or the extent to which any license under such rights
19 might or might not be available; neither does it represent that it has made any effort to
20 identify any such rights.

21 The IEEE-ISTO invites any interested party to bring to its attention any copyrights, patents,
22 or patent applications, or other proprietary rights which may cover technology that may be
23 required to implement the contents of this document. The IEEE-ISTO and its programs
24 shall not be responsible for identifying patents for which a license may be required by a
25 document and/or IEEE-ISTO Industry Group Standard or for conducting inquiries into the
26 legal validity or scope of those patents that are brought to its attention. Inquiries may be
27 submitted to the IEEE-ISTO by e-mail at: ieee-isto@ieee.org.

28 The Printer Working Group acknowledges that the IEEE-ISTO (acting itself or through its
29 designees) is, and shall at all times, be the sole entity that may authorize the use of
30 certification marks, trademarks, or other special designations to indicate compliance with
31 these materials.

32 Use of this document is wholly voluntary. The existence of this document does not imply
33 that there are no other ways to produce, test, measure, purchase, market, or provide other
34 goods and services related to its scope.

35

36 **About the IEEE-ISTO**

37 The IEEE-ISTO is a not-for-profit corporation offering industry groups an innovative and
38 flexible operational forum and support services. The IEEE-ISTO provides a forum not only
39 to develop standards, but also to facilitate activities that support the implementation and
40 acceptance of standards in the marketplace. The organization is affiliated with the IEEE
41 (<http://www.ieee.org/>) and the IEEE Standards Association (<http://standards.ieee.org/>).

42 For additional information regarding the IEEE-ISTO and its industry programs visit:

43 <http://www.ieee-isto.org>

44 **About the IEEE-ISTO PWG**

45 The Printer Working Group (or PWG) is a Program of the IEEE Industry Standards and
46 Technology Organization (ISTO) with member organizations including printer
47 manufacturers, print server developers, operating system providers, network operating
48 systems providers, network connectivity vendors, and print management application
49 developers. The group is chartered to make printers and the applications and operating
50 systems supporting them work together better. All references to the PWG in this
51 document implicitly mean “The Printer Working Group, a Program of the IEEE ISTO.” In
52 order to meet this objective, the PWG will document the results of their work as open
53 standards that define print related protocols, interfaces, procedures and conventions.
54 Printer manufacturers and vendors of printer related software will benefit from the
55 interoperability provided by voluntary conformance to these standards.

56 In general, a PWG standard is a specification that is stable, well understood, and is
57 technically competent, has multiple, independent and interoperable implementations with
58 substantial operational experience, and enjoys significant public support.

59 For additional information regarding the Printer Working Group visit:

60 <http://www.pwg.org>

61 Contact information:

62 The Printer Working Group
63 c/o The IEEE Industry Standards and Technology Organization
64 445 Hoes Lane
65 Piscataway, NJ 08854
66 USA
67

68 **About the Imaging Device Security Work Group (IDS)**

69 Description of PROJECT NAME.

70 For additional information regarding IDS visit:

71 <http://www.pwg.org/ids/>

72 Implementers of this specification are encouraged to join the IDS mailing list in order to
73 participate in any discussions of the specification. Suggested additions, changes, or
74 clarification to this specification, should be sent to the IDS Mailing list for consideration.

75

Table of Contents

76	
77	1. Introduction.....9
78	2. Terminology.....9
79	2.1 Conformance Terminology.....9
80	2.2 Other Terminology.....9
81	2.3 Acronyms and Organizations.....9
82	3. Requirements.....10
83	3.1 Rationale for IDS Identification, Authentication and Authorization.....10
84	3.2 Use Cases.....10
85	3.3 Out of Scope.....10
86	3.4 Design Requirements.....10
87	4. Security Elements.....11
88	4.1 Identification.....11
89	4.1.1 User Identification.....11
90	4.1.2 Client Identification.....11
91	4.1.3 Device Identification.....11
92	4.1.4 Service Identification.....11
93	4.2 Authentication.....11
94	4.3 Authorization.....11
95	5. Common Security Ticket Elements.....11
96	5.1 Authentication.....12
97	5.1.1 Token.....12
98	5.1.2 Certificate.....12
99	5.1.3 AuthenticationUri.....12
100	5.1.4 AuthenticationString.....12
101	5.1.5 UsernamePassword.....12
102	5.1.6 KeyInfo.....12
103	6. Security Elements.....12
104	6.1 UserSecurity.....12
105	6.1.1 UserIdentification.....13
106	6.1.2 UserAuthentication.....15
107	6.1.3 UserAuthorization.....15
108	6.2 Device Security.....15
109	6.2.1 DeviceIdentification.....16
110	6.2.2 DeviceAuthentication.....17
111	6.2.3 DeviceAuthorization.....17
112	6.3 Client Security.....18
113	6.3.1 ClientIdentification.....18
114	6.3.2 ClientAuthentication.....19
115	6.3.3 ClientAuthorization.....19
116	6.4 Service Security.....20
117	6.4.1 ServiceIdentification.....20
118	6.4.2 ServiceAuthentication.....21
119	6.4.3 ServiceAuthorization.....21
120	6.5 Job Security.....22

121	6.5.1 JobAuthentication	22
122	6.5.2 JobAuthorization	22
123	6.5.3 Document Security	23
124	7. Conformance Requirements	23
125	8. Internationalization Considerations	23
126	9. Security Considerations	23
127	10. IANA and PWG Considerations	24
128	11. References	24
129	11.1 Normative References	24
130	11.2 Informative References	24
131	12. Authors' Addresses	24
132	13. Change History	26
133	1. Introduction	7
134	2. Terminology	7
135	2.1 Conformance Terminology	7
136	2.2 Other Terminology	7
137	2.3 Acronyms and Organizations	7
138	3. Requirements	8
139	3.1 Rationale for Imaging Device Security Identification, Authentication and	
140	Authorization	8
141	3.2 Use Cases	8
142	3.3 Exceptions	8
143	3.4 Out of Scope	8
144	3.5 Design Requirements	8
145	4. Security Elements	9
146	4.1 Identification	9
147	4.1.1 User Identification	9
148	4.1.2 Client Identification	9
149	4.1.3 Device Identification	9
150	4.1.4 Service Identification	9
151	4.2 Authentication	9
152	4.3 Authorization	9
153	5. Common Security Ticket Elements	9
154	5.1 Authentication	9
155	5.1.1 Token	10
156	5.1.2 Cert	10
157	5.1.3 AuthUri	10
158	5.1.4 AuthString	10
159	5.1.5 UsernamePassword	10
160	5.1.6 KeyInfo	10
161	6. Security Elements	10
162	6.1 UserSecurity	10
163	6.1.1 User Identification	11
164	6.1.2 User Authentication	12
165	6.1.3 User Authorization	12

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted: Default Paragraph Font, Check spelling and grammar

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

Formatted

211	Figure 12 : Service Identification	20
212	Figure 13: Service Authorization	21
213	Figure 14: Job Security Elements.....	22
214	Figure 15: Job Authentication.....	22
215	Figure 16: Job Authorization.....	22
216	Figure 17: Document Security Elements.....	23
217	Figure 1: AuthenticationInfo Type	10
218	Figure 2: User Security Elements.....	10
219	Figure 3: User Identification	11
220	Figure 4: User Authorization	12
221	Figure 5: Device Security Elements	13
222	Figure 6: Device Identification	13
223	Figure 7: Device Authorization	14
224	Figure 8: Client Security Elements	15
225	Figure 9: Client Identification	15
226	Figure 10: Client Authorization	16
227	Figure 11: Service Security Elements	16
228	Figure 12 : Service Identification	17
229	Figure 13: Service Authorization	18
230	Figure 14: Job Security Elements.....	18
231	Figure 15: Job Authorization.....	18
232	Figure 16: Document Security Elements.....	19

List of Tables

No table of figures entries found.

238 **1. Introduction**

239 Provide an introduction for the document.

240 **2. Terminology**

241 **2.1 Conformance Terminology**

242 Capitalized terms, such as MUST, MUST NOT, RECOMMENDED, REQUIRED, SHOULD,
243 SHOULD NOT, MAY, and OPTIONAL, have special meaning relating to conformance as
244 defined in Key words for use in RFCs to Indicate Requirement Levels [RFC2119]. The
245 term CONDITIONALLY REQUIRED is additionally defined for a conformance requirement
246 that applies to a particular capability or feature.

247 **2.2 Other Terminology**

248 **2.3 Acronyms and Organizations**

249 *GPS*: Global Positioning System

250 *IANA*: Internet Assigned Numbers Authority, <http://www.iana.org/>

251 *IETF*: Internet Engineering Task Force, <http://www.ietf.org/>

252 *ISO*: International Organization for Standardization, <http://www.iso.org/>

253 *PWG*: Printer Working Group, <http://www.pwg.org/>

254

255

256 3. Requirements

257 3.1 Rationale for IDS Identification, Authentication and Authorization

258 Given the need for a standard method of defining, describing, and enforcing security for
259 Imaging Devices, the Imaging Device Security Identification, Authentication and
260 Authorization specification should:

- 261 1. Define new IDS Security Model element attributes and values to support
262 identification of Users, Imaging Devices, Jobs, and Documents.
- 263 2. Define new IDS Security Model element attributes and values to support
264 authentication of Users and Services.
- 265 3. Define new IDS Security Model element attributes and values to support Access
266 Control for Users, Services, Imaging Devices, Jobs, Designated Resources and
267 Documents.

Comment [JBM1]: Sync weith model rations

268 3.2 Use Cases

269 Add reference to the Model spec.

270 3.3 Out of Scope

271 The following are considered out of scope for this specification:

- 272 1. Definition of new security encryption protocols
- 273 2. Definition of new authentication methods
- 274 3. Definition of new security policy definition languages and formats

Comment [JBM2]: Sync with model

275 3.4 Design Requirements

276 The design requirements for this specification are:

- 277 1. Expand the IDS Security Model with new attributes and standard values to
278 support identification of Users, Devices, Imaging Devices, Service, Jobs, and
279 Documents~~users, printers, jobs, and documents,~~
- 280 2. Expand the IDS Security Model with new attributes and standard values to
281 support delegated resource access
- 282 3. Define example policies based on existing printing and imaging service
283 specifications
- 284 4. Define attributes and values for authentication, authorization, and access control
285 using existing protocols and schema.

Comment [JBM3]: Sync wioth model

286 | 5. Provide the ability for vendors to add extensions to the IAA values and attributes
287 | 3-6.

288 | **4. Security Elements**

289 | The IDS Identification, Authentication and Authorization specification defines core security
290 | attributes and values for three Imaging security areas: Identification, Authentication and
291 | Authorization. The IDS security attributes and values are assigned to one or more
292 | Security Actors (as defined in the IDS Security Model) and carried in a PWG Security
293 | Ticket.

294 | **4.1 Identification**

295 | **4.1.1 User Identification**

296 | The User Identification elements provide information to identify the User that is performing
297 | an operation.

298 | **4.1.2 Client Identification**

299 | The Client Identification elements provide identification information on any client processes
300 | or application that are being used in performing an operation.

301 | **4.1.3 Device Identification**

302 | The Device Identification elements identify the device that are used by a User or Client
303 | while performing an operation.

304 | **4.1.4 Service Identification**

305 | Service Identification elements are used to identify the service that is performing an
306 | operation.

307 | **4.2 Authentication**

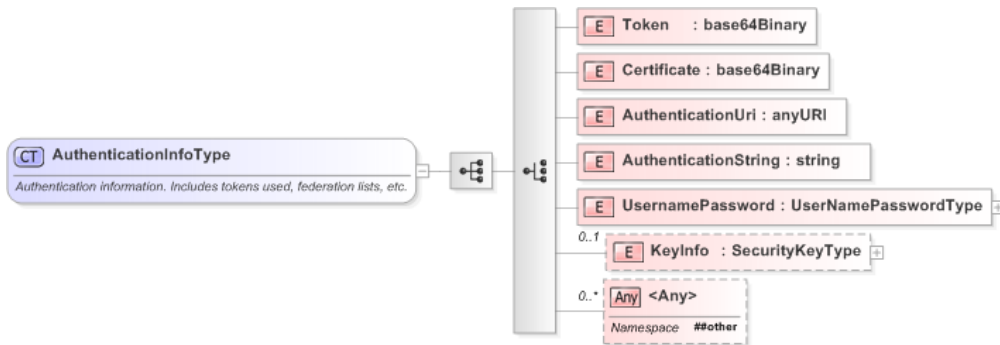
308 | **4.3 Authorization**

309 | **5. Common Security Ticket Elements**

310 | The following sets of security elements are common to all security actors and collections.

311 **5.1 Authentication**

312



313

314

Figure 1: AuthenticationInfo Type

315 **5.1.1 Token**

316 **5.1.2 Certificate**

317 **5.1.3 AuthenticationUri**

318 **5.1.4 AuthenticationString**

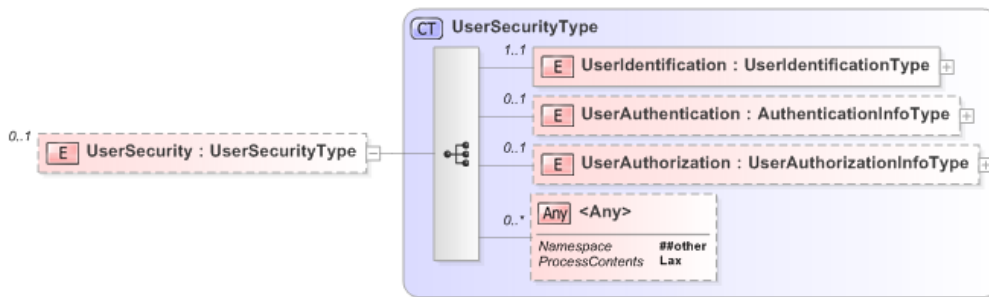
319 **5.1.5 UsernamePassword**

320 **5.1.6 KeyInfo**

321 **6. Security Elements**

322 **6.1 UserSecurity**

Comment [JBM4]: Add the scope for the issuer of the token



323

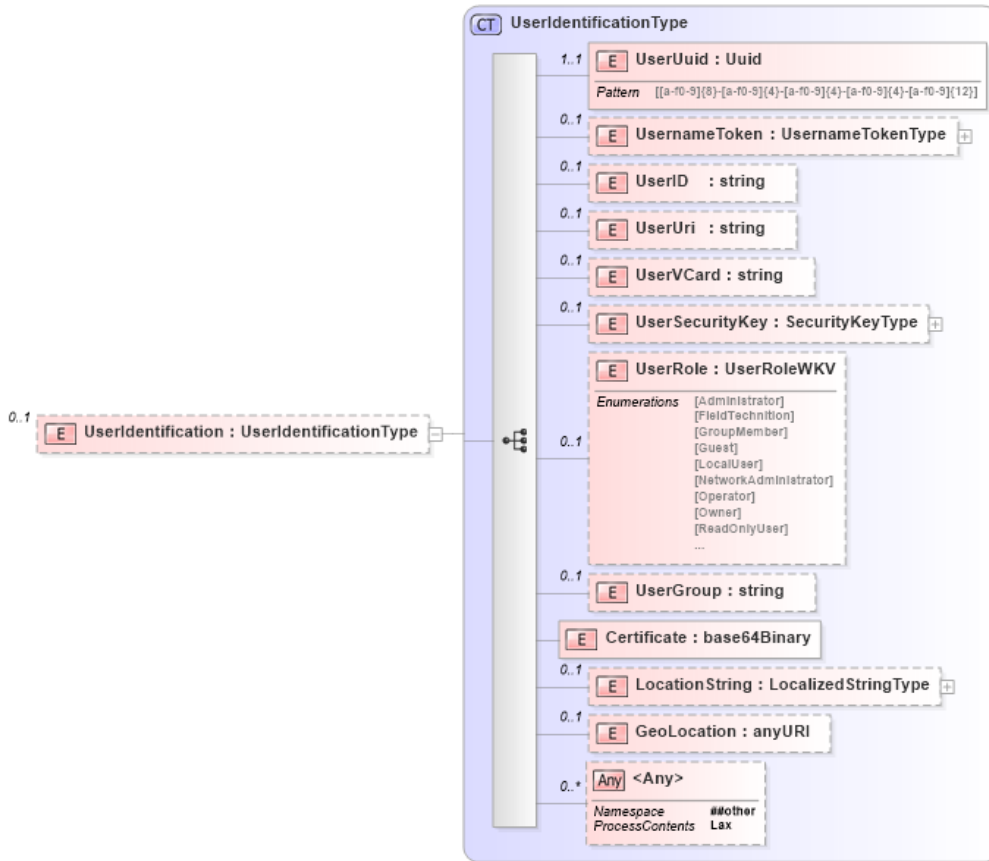
324

Figure 2: User Security Elements

325 | **6.1.1 User-Identification**

326 | The UserIdentification element contains the attributes necessary for identifying an User.

Comment [JBM5]: Breal location complex type into separate elements to match the Semantic Model



327

328

Figure 3: User Identification

329 | **6.1.1.1 UserUuid**

330 | A UUID value to uniquely identify the User. If a UUID is provided, it's value should be
331 | retained for the duration of any operation associated with the SecurityTicket

332 | **6.1.1.2 UsernameToken**

333 | The system Username associated with the User. This is typically the account name for the
334 | User

335 **6.1.1.3 UserId**

336 A system identification value assigned to the User account. This may be an account ID or
337 a user name

338 **6.1.1.4 UserUri**

339 A Uri value that identifies the User, such as an Email address

340 **6.1.1.5 UserVCard**

341 A VCard record that identifies the user.

Comment [JBM6]: RFC6351 and RFC6350
WebDAV6352

342 **6.1.1.6 UserSecurityKey**

343 A binary key, such as an OAuth or Active Directory Access token or Kerberos Ticket that
344 can be used to identify a User

345 **6.1.1.7 UserRole**

346 The User's role in an organization or within a system.

347 **6.1.1.8 UserGroup**

348 The organizational groups to which the User belongs

349 **6.1.1.9 Certificate**

350 An X509 Certificate that identifies the User

351 ~~6.1.1.9~~ **6.1.1.10 LocationString**

352 The LocationString element is a localized human-readable string describing the current
353 location of the user. This may be an abstract location value such as "In my car"

354 ~~6.1.1.10~~ **6.1.1.11 GeoLocation**

355 The Geolocation element represents the GPS coordinates of the current physical location
356 of the user. Generally this location will also refer to the location of the device the User is
357 actually using.

358 The coordinates MUST be expressed as specified in "A Uniform Resource Identifier for
359 Geographic Locations ('geo' URI)" ~~RFC5870~~ [RFC5870].

360 **6.1.2 User-Authentication**

361 **6.1.3 User-Authorization**

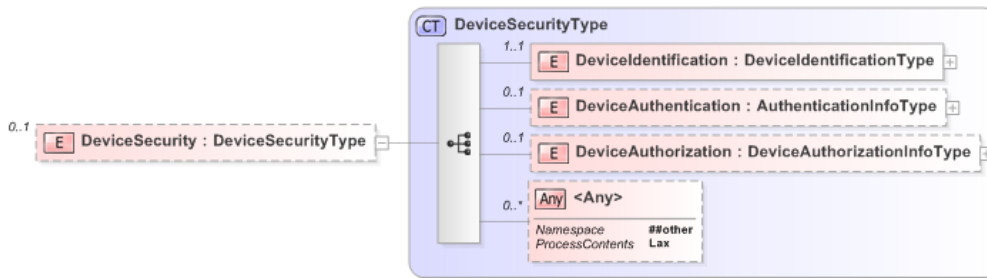


362

363

Figure 4: User Authorization

364 **6.2 Device Security**

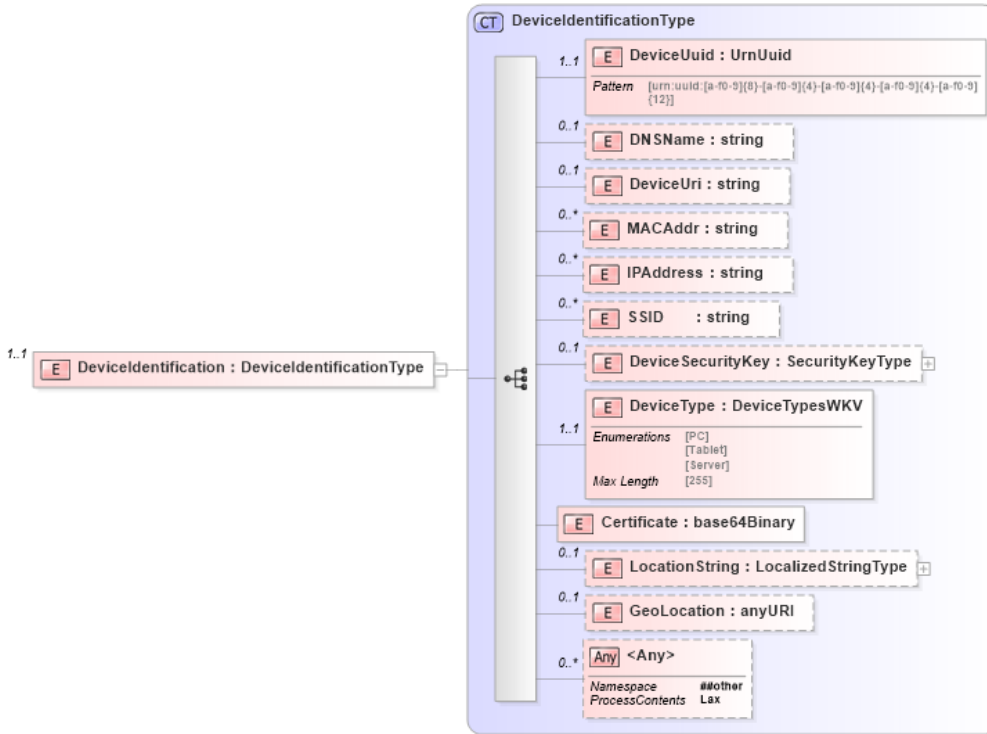


365

366

Figure 5: Device Security Elements

367 | **6.2.1 Device Identification**



368

369

Figure 6: Device Identification

370 The DeviceIdentification element contains the attributes necessary for identifying a Device.
371

372 **6.2.1.1 DeviceUuid**

373 A UUID value to uniquely identify the User. If a UUID is provided, the value MUST be
374 retained for as long as the Device is powered up. The value SHOULD be retained for the
375 lifetime of the Device.

376 **6.2.1.2 DNSName**

377 The registered DNS name of the Device

378 **6.2.1.3 DeviceUri**

379 | A Uri value that identifies the Device.

380 **6.2.1.4 MACAddr**

381 The Media Access Control (MAC) hardware addresses of the Device, one element for
382 each network interface

383 ~~6.2.1.4~~**6.2.1.5 IPAddr**

384 The IP Addresses of the Device, one element for each network interface

385 ~~6.2.1.5~~**6.2.1.6 DeviceSecurityKey**

386 A binary key, such as an X.509 Certificate or OAuth token that can be used to identify a
387 Device

388 ~~6.2.1.6~~**6.2.1.7 DeviceType**

389 A value identifying the type of the device

390 **6.2.1.8 Certificate**

391 An X509 Certificate that identifies the Device

392 ~~6.2.1.7~~**6.2.1.9 LocationString**

393 The LocationString element is a localized human-readable string describing the physical
394 location of the hardware device.

395 ~~6.2.1.8~~**6.2.1.10 GeoLocation**

396 The Geolocation element represents the GPS coordinates of the physical location of the
397 hardware device. The coordinates **MUST** be expressed as specified in RFC5870
398 [RFC5870].

399 **6.2.2 Device Authentication**

400 **6.2.3 Device Authorization**

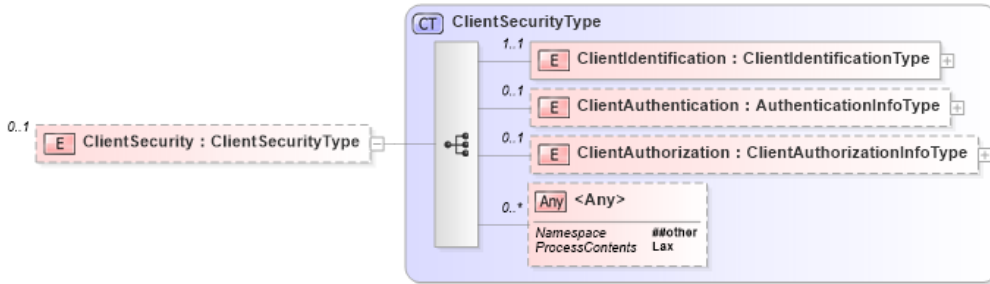


401

402

Figure 7: Device Authorization

403 **6.3 Client Security**

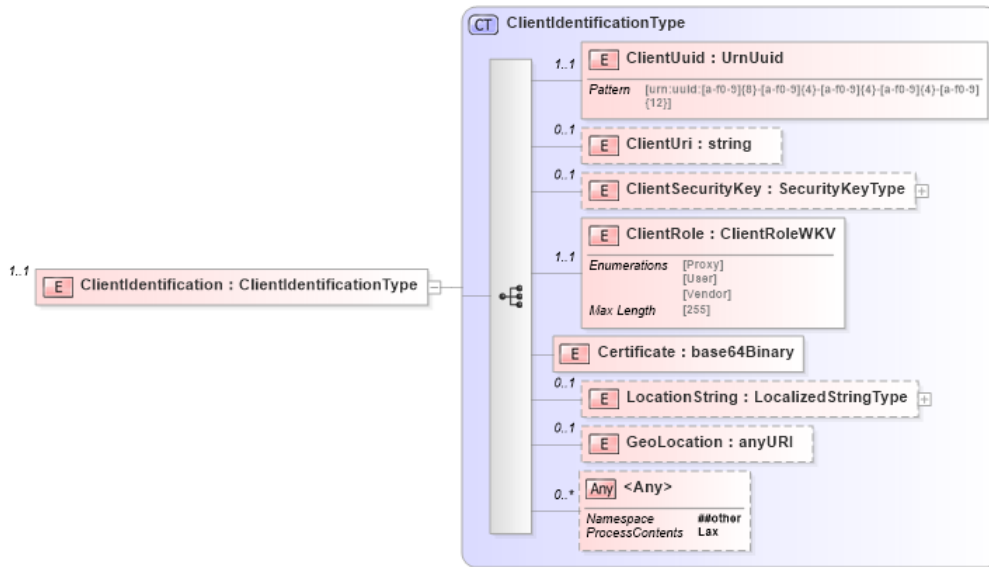


404

405

Figure 8: Client Security Elements

406 **6.3.1 Client-Identification**



407

408

Figure 9: Client Identification

409 The ClientIdentification element contains the attributes necessary for identifying a Client.

410

411 **6.3.1.1 ClientUuid**

412 A UUID value to uniquely identify the User. If a UUID is provided, the value MUST be
413 retained for the lifespan of the Client process or application.

414 **6.3.1.2 ClientUri**

415 A Uri value that identifies the Client process or application.

416 **6.3.1.3 ClientSecurityKey**

417 A binary key, such as an X.509 Certificate or OAuth token that can be used to identify a
418 Client process or application.

419 **6.3.1.4 ClientRole**

420 The role of the Client process

421 **6.3.1.5 Certificate**

422 An X509 Certificate that identifies the Client

423 ~~6.3.1.5~~ **6.3.1.6 LocationString**

424 The LocationString element is a localized human-readable string describing the physical
425 location of the hardware running service instance.

426 ~~6.3.1.6~~ **6.3.1.7 GeoLocation**

427 The Geolocation element represents the GPS coordinates of the physical location of the
428 hardware running service instance. The coordinates MUST be expressed as specified in
429 RFC5870 [RFC5870].

430 **6.3.2 Client-Authentication**

431 **6.3.3 Client-Authorization**

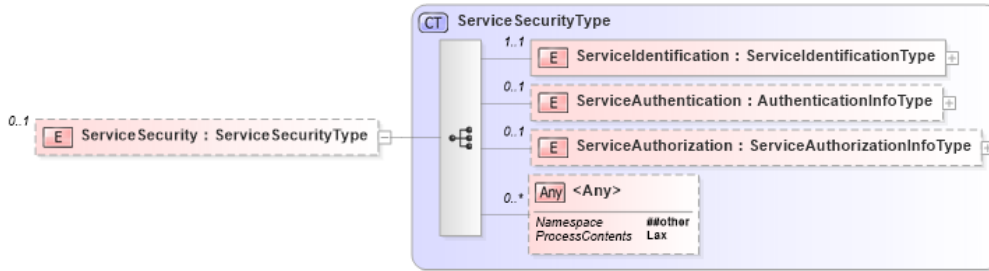


432

433

Figure 10: Client Authorization

434 **6.4 Service Security**

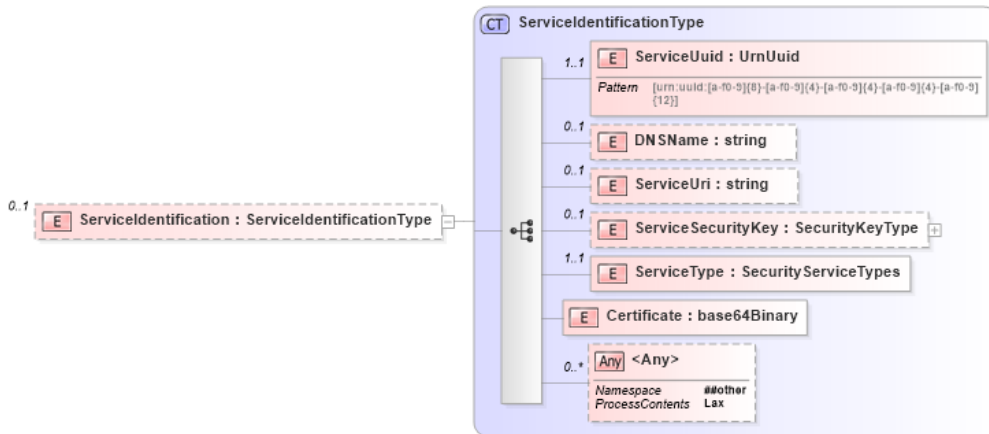


435

436

Figure 11: Service Security Elements

437 **6.4.1 Service Identification**



438

439

Figure 12 : Service Identification

440 The ServiceIdentification element contains the attributes necessary for identifying a
441 Service.

442

443 **6.4.1.1 ServiceUuid**

444 A UUID value to uniquely identify the User. If a UUID is provided, the value MUST be
445 retained for the lifespan of the Service instance. The value SHOULD be retained and the
446 same value used each time a specific instance of the service is executed.

447 **6.4.1.2 DNSName**

448 The DNS name entry for the Service

449 **6.4.1.3 ServiceUri**

450 A Uri value that identifies a Service instance.

451 **6.4.1.4 ServiceSecurityKey**

452 A binary key, such as an X.509 Certificate or OAuth token that can be used to identify a
453 Service instance.

454 **6.4.1.5 ServiceType**

455 A value identifying the type of Service

456 **6.4.1.6 Certificate**

457 An X509 Certificate that identifies the Service

458

459 ~~6.4.1.6~~ **6.4.1.7 LocationString**

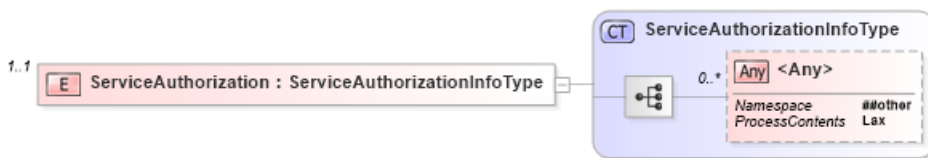
460 The LocationString element is a localized human-readable string describing the physical
461 location of the hardware running service instance.

462 ~~6.4.1.7~~ **6.4.1.8 GeoLocation**

463 The Geolocation element represents the GPS coordinates of the physical location of the
464 hardware running service instance. The coordinates MUST be expressed as specified in
465 RFC5870 [RFC5870].

466 **6.4.2 Service-Authentication**

467 **6.4.3 Service-Authorization**

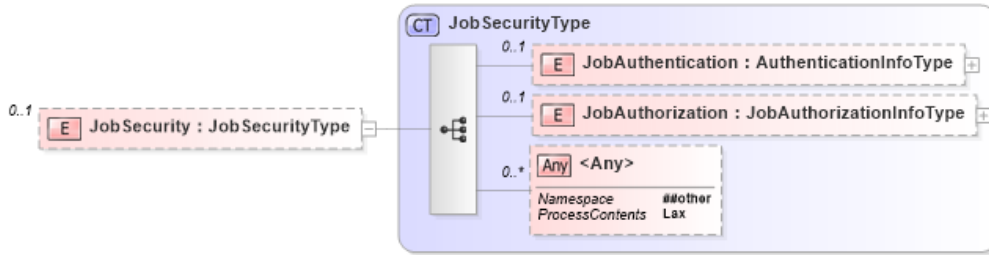


468

469

Figure 13: Service Authorization

470 **6.5 Job Security**

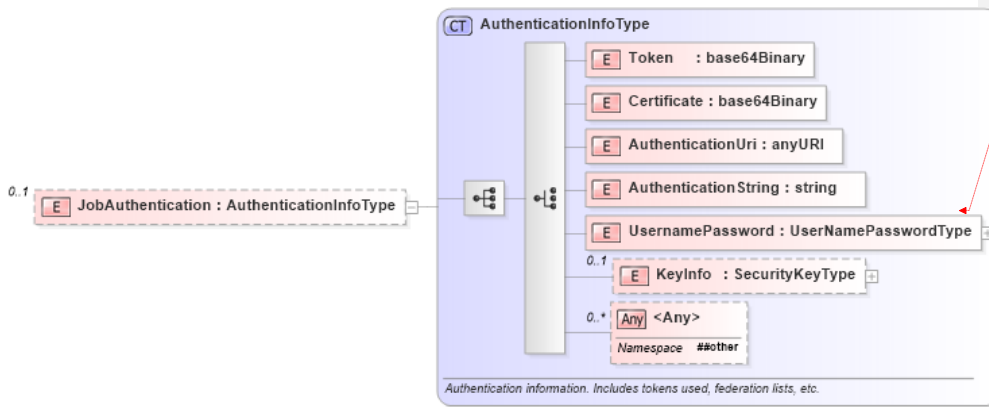


471

472

Figure 14: Job Security Elements

473 **6.5.1 Job-Authentication**



474

475

6.5.1 Figure 15: Job Authentication

476 **6.5.2 Job-Authorization**

477

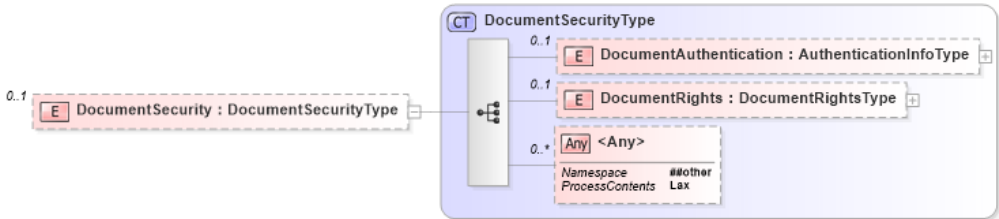


478

479

Figure 16: Job Authorization

480 **6.5.3 Document Security**



481

482

Figure 1746: Document Security Elements

483 **6.5.3.1 Document-Authentication**

484 The `DocumentAuthentication` element contains the authentication information necessary
485 for enable access to the document content. This information may range from a simple
486 document password to a document decryption token or key.

487 **6.5.3.2 Document-Rights**

488 The `DocumentRights` element contains the access and usage rights for the user, device or
489 service defined in a document operation.

490 General document rights information is carried in the document description and is defined
491 by Dublin core.

492 **7. Conformance Requirements**

493 Provide numbered lists of conformance requirements for the document.

494 **8. Internationalization Considerations**

495 For interoperability and basic support for multiple languages, conforming implementations
496 MUST support the Universal Character Set (UCS) Transformation Format -- 8 bit (UTF-8)
497 [RFC3629] encoding of Unicode [UNICODE] [ISO10646] and the Unicode Format for
498 Network Interchange [RFC5198].

499 **9. Security Considerations**

500 Applicable security considerations are described in the IDS Model Specification.
501 [IDSMODEL]

502 10. IANA and PWG Considerations

503 [This specification is consistent with the PWG Semantic Model Version 3.0 XML Schema](#)
504 [\[PWG-SCHEMA\]](#)

505 Provide IANA registration information for this [specification](#).

Comment [JBM7]: Point to schema location

506 Subsections include IANA registration templates using the Example style:

507 Some IANA registration text.

508 11. References

509 11.1 Normative References

510 [REFERENCE] F. Last author list or standards body, "Title of referenced document",
511 Document Number, Month YYYY, URL (if any)

512 [\[PWG-SCHEMA\]](#) [D. Manchala, "PWG Semantic Model V3.0 Schema",](#)
513 http://ftp.pwg.org/pub/pwg/sm3/schemas/PWG_SM_3.0_v2.904.zip

Field Code Changed

514 [RFC2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement
515 Levels", RFC 2119/BCP 14, March 1997,
516 <http://www.ietf.org/rfc/rfc2119.txt>

517 [RFC5870] A. Mayrhofer, C. Spanring, RFC 5870, "A Uniform Resource Identifier
518 for Geographic Locations ('geo' URI)", June 2010,
519 <http://www.ietf.org/RFC/RFC5870.txt>

520 11.2 Informative References

521 12. Authors' Addresses

522 Primary authors (using Address style):

523 Joe Murdock
524 Sharp Labs of America
525 5750 NW Pacific Rim Blvd
526 Camas, WA 98607
527 jmurdock@sharplabs.com

528 The authors would also like to thank the following individuals for their contributions to this
529 standard:

530 Nancy Chen
531 Michael Sweet - Apple
532 Ira McDonald - High North
533 Bill Wagner - TIC
534 Rick Yardumian - Canon
535

536 **13. Change History**

537 **13.1** April 2, 2011

Formatted: Font: Bold

Formatted: IEEEStd Paragraph

538 Initial revision.

539 **13.2** May 24, 2011

Formatted: Font: Bold

Formatted: IEEEStd Paragraph

540 Added Roles and Alerts.

541 **13.3** August 1, 2011

Formatted: Font: Bold

Formatted: IEEEStd Paragraph

542 Updated Security Ticket description and diagrams. Added Security operations.

543 **13.4** Oct 5, 2011

Formatted: Font: Bold

Formatted: IEEEStd Paragraph

544 Updated for schema changes. Added document security element.

545 **13.5** Feb 5, 2014

Formatted: Font: Bold

Formatted: IEEEStd Paragraph

546 Converted to new PWG template.

547 **13.6** Feb 5, 2014

Formatted: Font: Bold

Formatted: IEEEStd Paragraph

548 Updated for Schema changes. Added description of Identification elements. Major
549 reorganization.

550 **November 1, 2014**

551 Updated for Schema changes.

552